

THE DANGER OF FACIAL RECOGNITION IN OUR CHILDREN'S CLASSROOMS

NILA BALA[†]

ABSTRACT

The use of facial recognition in classrooms to monitor students' performance is already happening in China and soon may be coming to the West. Surveilling students in their classrooms presents a number of potential harms: (1) it implicates their privacy, (2) it could have profound effects on their development and stigmatizes youth who develop differently, and (3) it might amplify current inequities in our school system. Additionally, there are societal harms from this practice to our democratic society. To the extent that educators wish to employ this technology, our current legal regime is inadequate to mitigate the harms. While some changes could be made to better protect privacy and equity, ultimately, lawmakers and schools should consider banning facial recognition within classrooms.

INTRODUCTION

Schools in China have recently reported using facial recognition to monitor how attentive students are in the classroom.¹ Cameras are installed above the blackboard and, by identifying facial expressions, the system determines whether children are focused on their lessons.² If not, the computer feeds this information back to the teacher who grades the students accordingly.

The use of facial recognition technology in the classroom may soon be coming to the West. Americans are already contemplating its use here. Researchers at North Carolina State University have recorded students' faces while they were using a computer coding tutorial to

[†] Associate Director of Criminal Justice Policy, R Street Institute. J.D. 2012, Yale Law School; B.A. 2008, Stanford University. The views expressed in this article are solely those of the author and not of R Street Institute.

¹ Xinmei Shen, *China is Putting Surveillance Cameras in Plenty of Schools*, TECH IN ASIA (Jan. 22, 2019), <https://www.techinasia.com/china-putting-surveillance-cameras-plenty-schools>.

² Rachel England, *Chinese School Uses Facial Recognition to Make Kids Pay Attention*, ENGADGET (May 17, 2018), <https://www.engadget.com/2018/05/17/chinese-school-facial-recognition-kids-attention/>.

determine who was having trouble with the material.³ In New York, a company named SensorStar Labs is monitoring children using a facial recognition software called EngageSense, which applies algorithms to interpret the students' levels of engagement.⁴ Schools have already purchased facial recognition technology for security reasons.⁵ These cameras could also be used to monitor student performance.⁶

As facial recognition technology improves, privacy fears expand accordingly. These fears include legitimate concerns about how data will be collected, categorized, and stored. But there is also a separate issue related to the effects of using facial recognition to surveil classroom engagement on children's still-developing minds. So far, the technology has generally been described in a beneficial manner—as motivating the wandering minds of students to stay focused and providing teachers with valuable feedback about how well students are learning. Surveillance of children, however, can have a profound effect on their development and on their privacy expectations later in life.⁷ Additionally, facial recognition in classrooms can stigmatize differing abilities to focus and might even amplify the school-to-prison pipeline. Ultimately, surveillance has adverse consequences: by monitoring children in their place of learning, we undermine a free society.

I. BACKGROUND

Surveillance threatens the rights that constitute a functioning democracy—including the rights to speak, think, assemble, and vote without being watched. Some level of anonymity is key to being able to protest corruption and challenge the state. A study of high-surveillance

³ Kecia Lynn, *Bringing Facial Recognition Software Into The Classroom*, BIG THINK (July 1, 2013), <https://bigthink.com/ideafeed/bringing-facial-recognition-software-into-the-classroom>.

⁴ Randy Rieland, *Can Facial Recognition Really Tell If a Kid Is Learning in Class?*, SMITHSONIAN MAG. (Nov. 1, 2013), <https://www.smithsonianmag.com/innovation/can-facial-recognition-really-tell-if-a-kid-is-learning-in-class-8163550/#dcdIHLrADPjuCixb.99>.

⁵ Ava Kofman, *Face Recognition is Now Being Used in Schools, but It Won't Stop Mass Shootings*, THE INTERCEPT (May 30, 2018), <https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/>.

⁶ Robert D. Bickel et. al., *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in A Democracy, or Will the Courts Strike A Proper Balance?*, 33 STETSON L. REV. 299, 305 (2003) (discussing how security cameras can also be used to monitor workplace performance).

⁷ OFFICE OF THE PRIVACY COMM'R OF CAN., SURVEILLANCE TECHNOLOGIES AND CHILDREN: REPORT PREPARED BY THE RESEARCH GROUP OF THE OPC 5–7 (2012).

states demonstrates its costs. In the former German Democratic Republic, for example, the Stasi would spy extensively on its populace, singling out subversive individuals.⁸ By utilizing a network of informants, including friends and family members, the Stasi collected the most intimate information on persons of interest, bugging their homes and offices. The effect in Germany at the time was self-censorship.⁹ The backlash now is vehement opposition—higher than rates in any other Western country, Germans oppose government surveillance.¹⁰ Similarly, in present-day China, 176 million cameras (with that number rapidly expected to expand in the coming years) track citizens' movement in order to facilitate the monitoring and punishing of critics, dissidents, and human rights activists alike.¹¹ The government is developing "citizen scores."¹² Anti-government activity (or even associating with those who have posted anti-government messages) can lower scores.¹³ One's citizen score may determine one's access to certain privileges, such as the ability to travel.¹⁴ Surveillance quashes intellectual freedom, disrupts relationships, and changes the culture in states implementing its use. It fundamentally changes the way individuals think and act, and causes them to avoid speaking or writing about controversial subjects or expressing dissent.¹⁵

Surveillance is not just about being watched, but about who is watching. The most common counter to surveillance is a call to protect privacy, but privacy is not the only issue with surveillance.¹⁶ In actuality, surveillance is a relationship built on differing power dynamics, with

⁸ Thomas Coombes, *Lessons from the Stasi: A Cautionary Tale on Mass Surveillance*, AMNESTY INT'L (Mar. 31, 2015),

<https://www.amnesty.org/en/latest/news/2015/03/lessons-from-the-stasi/>.

⁹ Peter Wensierski, *East German Snitching Went Far Beyond the Stasi*, SPIEGEL ONLINE (July 10, 2015), <https://www.spiegel.de/international/germany/east-german-domestic-surveillance-went-far-beyond-the-stasi-a-1042883.html>.

¹⁰ See Coombes, *supra* note 8.

¹¹ Anna Mitchell & Larry Diamond, *China's Surveillance State Should Scare Everyone*, ATLANTIC (Feb. 2, 2018),

<https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/>.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Jonathan Shaw, *The Watchers: Assaults on Privacy in America*, HARVARD MAG. (Jan.–Feb. 2017), <https://harvardmagazine.com/2017/01/the-watchers>.

¹⁶ See Felix Stalder, *Privacy is Not the Antidote to Surveillance*, 1 SURVEILLANCE & SOC'Y 120, 120–24 (2002), <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3397>.

those in power having the ability to possess and control information. With the state as the “watcher,” it is easy to see how there would be an inherent power imbalance between the state and the individual. Additionally, history indicates that the state does not wield its power equitably against its citizens. Scholars, such as Alvaro Bedayo, Dorothy Roberts, and Jeffrey Vogle, have noted that state actors have historically used surveillance against minorities and immigrants as a form of social control.¹⁷

Similarly, children suffer from a power imbalance—one that legal academics have generally not scrutinized.¹⁸ Children lack full rights and responsibilities and have less power and control over their lives than adults. Due to this minority status and relative lack of development, however, this power imbalance is deemed appropriate. One model stipulates that children’s rights are “held in trust” for them: children are full citizens but with some rights preserved by adults, to be exercised in the future.¹⁹ The adults who hold these rights in trust are to consider how the decisions made during the child’s minority will affect both the child’s current and future welfare.²⁰ The assumption is that, despite the power imbalance between children and adults, those in charge will act in the children’s best interest.

Perhaps those in favor of facial recognition in classrooms may raise the argument that children are different from adults, and because of their minority status, do not need or deserve privacy. In reality, young people do have a right to privacy, which grows as they age and their capabilities evolve. The highest court has recognized that this right extends, at least in some contexts, to children.²¹ While privacy has many

¹⁷ Alvaro Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html; Dorothy Roberts & Jeffrey Vagle, *Racial Surveillance Has a Long History*, THE HILL (Jan. 4, 2016), <https://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history>.

¹⁸ Annette Ruth Appell, *Accommodating Childhood*, 19 CARDOZO J.L. & GENDER 715, 715 (2013).

¹⁹ Connie K. Beck et al., *Rights of Children: A Trust Model*, 46 FORDHAM L. REV. 669, 696 (1978).

²⁰ *See id.* (explaining how these adults would have the duties of a trustee).

²¹ *See, e.g.,* Bellotti v. Baird, 443 U.S. 622, 643 (1979) (mandating that, if a state requires parental consent for a minor obtaining an abortion, “it also must provide an alternative procedure whereby authorization for the abortion can be obtained”) (internal citations omitted); Carey v. Population Servs. Int’l, 431 U.S. 678, 693 (1977) (“[T]he right to privacy in connection with decisions affecting procreation extends to minors as well as to adults.”); Planned Parenthood v.

definitions, perhaps the most famous one was articulated by Samuel Warren and Louis Brandeis in their seminal *Right to Privacy*²² article. They frame privacy as the right to be left alone and to be free of outside interference.²³ As children develop into adolescents, privacy, the right to develop their identity in spaces that are truly theirs without being watched, becomes vital to their growth and development. Yet children's privacy is often put aside in favor of security or safety, even when the two values can safely coexist.²⁴ Even when there is no safety issue, children's privacy is often disregarded.²⁵

Most adults would not tolerate being spied on in their analogue to the classroom—the workplace. When surveyed, most American adults do not like the idea of surveillance on their activities and want to do more to protect their privacy.²⁶ Even if employers can legally monitor much of their employees' behaviors on employer-owned devices, employees have actively resisted facial recognition for monitoring their productivity and focus in the workplace.²⁷ The National Union of Journalists expressed outrage when a UK Newspaper, the *Daily Telegraph*, positioned “OccupEye” sensors under employees' desks to track attendance under the pretense of gathering energy-efficiency data.²⁸ Because of the outcry, the project ultimately ceased.²⁹

Danforth, 428 U.S. 52, 74 (1976) (holding that a state “may not impose a blanket provision requiring the consent of a parent . . . as a condition for abortion of an unmarried minor during the first 12 weeks of her pregnancy” in order to protect their right of privacy).

²² Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

²³ “Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term ‘property’ has grown to comprise every form of possession—intangible, as well as tangible.” *Id.* at 193.

²⁴ Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 761 (2011).

²⁵ *Id.*

²⁶ Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014),

<http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

²⁷ See Lewis Maltby, *Employment Privacy: Is There Anything Left?*, 39 HUM. RTS. MAG. 12, 12 (2013).

²⁸ Ben Quinn & Jasper Jackson, *Daily Telegraph to Withdraw Devices Monitoring Time at Desk After Criticism*, GUARDIAN (Jan. 11, 2016), <https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to-withdraw-devices-monitoring-time-at-desk-after-criticism>.

²⁹ *Id.*

Even if the *Daily Telegraph* had not terminated the project, the adult employees involved would have had both the choice and the leverage that children lack: if adults find employer surveillance too repugnant, they can leave their job or at least threaten to do so. Yet adults seem ready to subject children in the classroom to a level of surveillance that they do not want for themselves, contending that doing so is in the children's best interest.

Surveillance's benefit is also advertised as improving children's academic performance. Even that claim, however, must be scrutinized. Classroom facial recognition poses potential harms by stigmatizing some normal behaviors and punishing children who may not be neurotypical.³⁰ The technology assumes that attention deficits are under conscious control, which is not the case. Even when an individual is intent on focusing, psychologists have found that unintentional wandering thoughts normally occur.³¹ Similarly, children who do not display eye contact or the facial expressions the algorithm favors may have non-neurotypical ways of learning, meaning their lack of eye contact and inattentive facial expressions do not necessarily indicate that they are exhibiting "negative" behaviors or not learning. If performance is just based on eye contact and other facial indicators, facial recognition software cannot distinguish between intentional and unintentional mind-wandering, nor can it account for expressions of non-neurotypical children.

Additionally, there may be benefits to mind-wandering. Children whose minds wander may actually have larger working memories and display more creativity than those who do not tend to daydream.³² Robert Sapolsky, a neuroendocrinologist at Stanford University, has identified mind-wandering as an incredibly beneficial exercise.³³ When the mind wanders, it has a chance to engage in creative problem solving, imagining future scenarios and how they might turn out.³⁴ Additionally,

³⁰ Chaunie Brusie, *All About Recognizing a Neurotypical*, HEALTHLINE (June 28, 2017), <https://www.healthline.com/health/neurotypical> (defining neurotypical as "individuals of typical developmental, intellectual, and cognitive abilities").

³¹ Peter Reuell, *When Wandering Minds Are Just Fine*, MINDFUL (June 27, 2018), <https://www.mindful.org/when-wandering-minds-are-just-fine/>.

³² See THE TELEGRAPH, *Children Whose Minds Wander 'Have Sharper Brains'* (Mar. 16, 2012), <https://www.telegraph.co.uk/news/science/9149684/Children-whose-minds-wander-have-sharper-brains.html>.

³³ Robert Sapolsky, *The Benefits of Mind-Wandering*, WALL ST. J. (June 19, 2015), <https://www.wsj.com/articles/the-benefits-of-mind-wandering-1434716243>.

³⁴ *Id.*

mind-wandering can be protective. Mind-wandering helps distract children and adults from the temptation of giving up on tedious tasks, thereby permitting them to complete tasks successfully.³⁵

The disdain toward mind-wandering in children is reminiscent of an old view of children's play once seen as a wasteful part of childhood. Under this puritanical view, children are born evil, with frivolity, and play seen as evil.³⁶ We now know that play is vital for physical and mental development.³⁷ Mind-wandering has similar benefits related to creativity.³⁸ But even without a clear tangible benefit, both play and mind-wandering hold a special, sacred place in what makes us human and, more specifically, in what defines childhood.

II. EFFECTS OF SURVEILLANCE ON CHILDREN

Surveillance is not beneficial for children. Not only does it discourage mind-wandering and creativity, but it also works against children becoming autonomous, fully functional citizenry. We uphold freedom as one of the paramount American values, yet we are unwilling to allow children to explore its bounds. Unlike adults, children are still in the midst of growth and development, which makes them particularly vulnerable to the effects of emerging technology, including mass surveillance. One study has shown that children as young as 18 months are aware when they are being watched, and it can change their behavior and development.³⁹ Science further continues to reveal how the prefrontal cortex—the part of the brain that controls impulses and reasoning—continues to develop from childhood through adolescence and early adulthood. Even the Supreme Court, in formulating its jurisprudence of how children should be treated in the criminal justice system, has repeatedly emphasized the differences between children and

³⁵ See Jonathan Smallwood et al., *Letting Go of the Present: Mind-Wandering Is Associated with Reduced Delay Discounting*, 22 CONSCIOUSNESS & COGNITION 1, 5 (2012).

³⁶ HOWARD P. CHUDACOFF, *CHILDREN AT PLAY: AN AMERICAN HISTORY* 19 (2007).

³⁷ Kenneth R. Ginsburg, *The Importance of Play in Promoting Healthy Child Development and Maintaining Strong Parent-Child Bonds*, 119 PEDIATRICS 182, 182 (2007) (“Play is so important to optimal child development that it has been recognized by the United Nations High Commission for Human Rights as a right of every child.”).

³⁸ See Sapolsky, *supra* note 33.

³⁹ Adam Bisby, *When Does Protecting Your Child Become Invasion of Privacy?*, GLOBE AND MAIL (Feb. 21, 2004), <https://www.theglobeandmail.com/life/parenting/when-does-protecting-your-child-become-invasion-of-privacy/article17041213/>.

adults.⁴⁰ It is during childhood that the ability to focus and think critically is cemented. Therefore, psychological harms from technology's surveillance may have a greater and more lasting effect on children than on adults because of the "many social, biological, cognitive, and psychological changes that characterize this life period."⁴¹

Valuing surveillance above autonomy can result in heteronomy: "the condition of being governed by someone else."⁴² Researchers have found that heteronomous children can have difficulties with tasks that require critical thinking and become overly reliant on parents, teachers, and the state to make decisions for them.⁴³ When they do make decisions, heteronomous children report making the "right" decision because they are being watched, rather than as a result of their own discernment of what decision is the correct or moral one.⁴⁴ For example, these children reported that lying was wrong only if they were punished.⁴⁵ Furthermore, they indicated that lying to adults was worse than lying to children because adults would know if they were lying.⁴⁶ Surveillance takes away children's ability to grow into meaningfully engaged adults by overly scrutinizing their behavior. Compounded over many individuals, surveillance takes away a discerning citizenry, which is key to a functioning democracy.

⁴⁰ See *United States Supreme Court Juvenile Justice Jurisprudence*, NAT'L JUV. RESOURCE CTR.,

<http://njdc.info/practice-policy-resources/united-states-supreme-court-juvenile-justice-jurisprudence/> (last accessed Oct. 27, 2019). For example, the Court stated that juveniles display a "lack of maturity and an underdeveloped sense of responsibility are found in youth more often than in adults." *Roper v. Simmons*, 543 U.S. 551, 569 (2005) (internal citations and quotations omitted).

Additionally, the Court noted that "developments in psychology and brain science continue to show fundamental differences between juvenile and adult minds." *Graham v. Florida*, 560 U.S. 48, 68 (2010).

⁴¹ Daniel Kardefelt-Winther, *How Does the Time Children Spend Using Digital Technology Impact Their Mental Well-Being, Social Relationships and Physical Activity?*, UNICEF (Dec. 2017), <https://www.unicef-irc.org/publications/pdf/Children-digital-technology-wellbeing.pdf> ("Even though adults also use digital technology to a great extent, concerns tend to cent[er] on children's use because of the many social, biological, cognitive, and psychological changes that characterize this life period.").

⁴² Jason Nolan et al., *The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media*, 36 CANADIAN CHILD. J. 24, 26 (2011).

⁴³ *Id.* at 25–26.

⁴⁴ *Id.* at 26.

⁴⁵ *Id.*

⁴⁶ *Id.*

III. SURVEILLANCE AND INEQUITY

Unfortunately, not all children are likely to be monitored in the same way. Current inequities within the classroom start as early as preschool, where black children are viewed as criminal (rather than childlike) early on.⁴⁷ Studies have found that black children, relative to their white counterparts, are disproportionately suspended as preschoolers.⁴⁸ Children with disabilities also suffer from disproportionate suspensions.⁴⁹ Suspensions only exacerbate learning gaps and create more opportunities for children to engage in criminal conduct and enter the juvenile justice system.⁵⁰

Surveillance is already employed as a tool to punish misbehavior, specifically targeting children of color. In the wake of the Sandy Hook Elementary shooting, many schools enhanced their surveillance procedures, but not at equal rates.⁵¹ Schools with a majority of students of color were far more likely to include more surveillance.⁵² Professor Jason Nance, the researcher who conducted the study, concluded that “schools with higher concentrations of minority students are more inclined to rely on heavy-handed measures to maintain order than other schools facing similar crime and discipline issues.”⁵³

Human biases have also pervaded the machine learning that facial recognition technology employs. A recent study identified that facial recognition is much worse at identifying people of color and women as compared to white men.⁵⁴ Technology is seen as immune to the racial biases that humans possess, and individuals view artificial intelligence with blind faith. But artificial intelligence is only as smart as

⁴⁷ See generally Phillip Atiba Goff et al., *The Essence of Innocence: Consequences of Dehumanizing Black Children*, 106 J. PERSONALITY & SOC. PSYCHOL. 526 (2014).

⁴⁸ OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF EDUC., CIVIL RIGHTS DATA COLLECTION: DATA SNAPSHOT: (SCHOOL DISCIPLINE) (Mar. 21, 2014), <https://www2.ed.gov/about/offices/list/ocr/docs/crdc-discipline-snapshot.pdf>.

⁴⁹ *Id.*

⁵⁰ Alison Evans Cuellar & Sara Markowitz, *School Suspension and the School-to-Prison Pipeline*, 43 INT'L REV. L. & ECON. 98, 98–106 (2015), <https://www.sciencedirect.com/science/article/abs/pii/S014481881500040X>.

⁵¹ Jason P. Nance, *Student Surveillance, Racial Inequalities, and Implicit Racial Bias*, 66 EMORY L.J. 765, 800–01 (2017).

⁵² *Id.* at 800–16.

⁵³ *Id.* at 811.

⁵⁴ Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>.

the data used to develop it. If children of color are not identified correctly in the classroom, how can they be evaluated fairly?

Even with the most well-meaning of teachers and administrators acting in good faith, there is a reasonable concern that the burdens of facial recognition in classrooms will fall most heavily on minority students. Implicit bias has remained a persistent problem in schools.⁵⁵ It is not a far stretch to imagine that facial recognition will provide another tool to police children of color, that facial recognition will be applied inequitably across or within classrooms, and that children of color will disproportionately pay the price of systems that punish mind-wandering.

IV. LEGAL FRAMEWORK

There are benefits to surveillance, and we are glad it exists in areas like banks. However, surveillance also comes at a cost to a free society. A pragmatic legal approach is to come up with regulations that would operate like guardrails, while recognizing that the technology already exists and is being used for other purposes. In the United States, cameras with facial recognition already exist in schools for security purposes. Putnam City Schools in Oklahoma recently announced that they will be using facial recognition to target a short list of suspects (so far, not students).⁵⁶ In Detroit, Gibraltar Public Schools also have new digital security cameras that utilize facial recognition to track all individuals entering.⁵⁷ While security cameras are for a different use than school performance in the classroom, some of the policy solutions proposed below to protect privacy would still apply. Additionally, we can still take the stand that facial recognition should not be used for purposes beyond its current one.

⁵⁵ Laura R. McNeal, *Managing Our Blind Spot: The Role of Bias in the School-to-Prison Pipeline*, 48 ARIZ. ST. L.J. 285, 285–86 (2016) (“[O]verly harsh school disciplinary practices and excessive use of force are imposed more frequently on African American and Latino students, than their white peers. This disparity is largely due to the failure to address the influence of explicit and implicit biases in school disciplinary decisions and the continued use of draconian school disciplinary practices.”).

⁵⁶ Kaitlyn DeHaven, *Oklahoma District Uses Facial Recognition to Secure Campuses*, CAMPUS SECURITY & LIFE SAFETY (Aug. 13, 2019), <https://campuslifesecurity.com/articles/2019/08/13/oklahoma-district-uses-facial-recognition-to-secure-campuses.aspx>.

⁵⁷ John Wisely, *School Security Cameras Add Facial Recognition Software*, DETROIT FREE PRESS (Aug. 12, 2019), <https://www.freep.com/story/news/education/2019/08/12/michigan-schools-beef-up-security/1942553001/>.

As a threshold matter, we may decide as a democratic society that, regardless of any benefits, this technology holds too many harms to be considered. To the extent we wish to allow it in a limited manner, there are three areas the law might address. First, there are privacy concerns: for example, who might have access to facial recognition data, how it is collected, and stored. Second, the disparities in surveillance raise concerns of equity and how this technology might be used in the fairest way possible. Finally, facial recognition might affect child development in a damaging way. I consider each category below in turn, but ultimately recommend, that to protect childhood as we know it, facial recognition in classrooms should be rejected.

(1) Privacy

School children have a legitimate right to privacy on school grounds. The law has limited this right to balance a school's need to maintain a safe learning environment. As an initial matter, students likely do not have a constitutional claim under the Fourth Amendment to prevent the implementation of cameras in classrooms. In a number of cases, video surveillance in classrooms and public spaces in schools has been found to be reasonable since the classroom does not fall within a protected "zone of privacy" where individuals would have reasonable expectations that they will not be surveilled.⁵⁸ Classrooms, unlike locker rooms and bathrooms, are public spaces.⁵⁹

Still, to the extent surveillance footage is collected for school performance purposes, one potential avenue for protecting some privacy rights is the Family Educational Rights and Privacy Act ("FERPA").⁶⁰ FERPA protects information that falls within its definition of a "student education record."⁶¹ An education record under FERPA is information "maintained by [the student's] educational agency or institution or by a person acting for such agency or institution" that is "directly related to [the] student."⁶² Education records can include media, such as video

⁵⁸ The U.S. Supreme Court first acknowledged that the Bill of Rights created a "zone of privacy" meaning in *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) ("Various guarantees create zones of privacy."). These implied rights create zones—such as marriage and the home—in which the government should not intrude. *Id.* at 486.

⁵⁹ See *Roberts v. Hous. Indep. Sch. Dist.*, 788 S.W.2d 107, 111 (Tex. App. 1990) (holding that the activity of teaching at a public school did not fall within the zone of privacy). *But see* *Brannum v. Overton Cty. Sch. Bd.*, 516 F.3d 489 (6th Cir. 2008) (holding that a school locker room was within the zone of privacy).

⁶⁰ 20 U.S.C. § 1232g (2012).

⁶¹ *Id.*

⁶² § 1232g(a)(4)(A).

recordings.⁶³ There has been considerable debate, however, on whether video recordings for surveillance and security purposes can be education records.⁶⁴ On the other hand, video recordings in classrooms for the purpose of evaluating a student's performance seems to fit more squarely into the definition of an education record, and FERPA specifies that it applies to biometric information, like facial recognition.

To be clear, nothing in FERPA regulates or prevents the use of facial recognition in classrooms. FERPA, however, helps to effectively prevent the dissemination of educational records and provides parents and adult students the right to inspect their records. Since facial recognition data is likely part of an educational record, it would be protected in the same way as other forms of educational data. Schools would be required to ask for consent before disclosing data to individuals other than parents or school officials. Unfortunately, FERPA does not provide guidance for regulating how data is stored and managed. This is particularly a concern, as student data might be shared on the cloud with outside service providers.

An additional statute to consider is the Child Online Privacy Protection Act ("COPPA"), which mandates commercial websites, online services, and mobile apps notify parents and obtain their consent before collecting any personal information on children under the age of thirteen.⁶⁵ COPPA does not apply to governmental agencies, however, including schools.⁶⁶ COPPA also falls short because it applies to information collected from children rather than about children.⁶⁷

⁶³ 34 C.F.R. § 99.3 (2013).

⁶⁴ See, e.g., U.S. DEP'T OF EDUC., BALANCING STUDENT PRIVACY AND SCHOOL SAFETY: A GUIDE TO THE FAMILY AND EDUCATIONAL RIGHTS AND PRIVACY ACT FOR ELEMENTARY AND SECONDARY SCHOOLS (2007), <http://www.ed.gov/policy/gen/guid/fpco/brochures/elsec.pdf> (clarifying that the U.S. Department of Education considers exempt from FERPA law enforcement unit records, security video, and even education records when they are used to "protect the health or safety of students or other individuals").

⁶⁵ See 15 U.S.C. § 6501(1) (defining the term "child" to mean "an individual under the age of 13").

⁶⁶ *Id.*; see also Benjamin Herold, *COPPA and Schools: The (Other) Federal Student Privacy Law, Explained*, EDUC. WK. (July 28, 2017), <https://www.edweek.org/ew/issues/childrens-online-privacy-protection-act-coppa/index.html> ("This law directly regulates companies, not schools.").

⁶⁷ See Herold, *supra* note 66 ("It's worth noting that COPPA applies only to information that is collected *from* children, not to information that is collected *about* children."). Additionally, within the statutory language of COPPA "from children" is used 19 times, while "about children" is mentioned in the title, but never again.

Therefore, depending on how facial recognition data is categorized, COPPA may not apply. Thus, FERPA and COPPA neither prevent nor adequately regulate facial recognition in classrooms.

Even model legislation on facial recognition technology, such as the one proposed by Georgetown Law School's Privacy and Technology Center, is specific to law enforcement's collection of facial recognition information and does not address schools.⁶⁸ Similarly, a bipartisan bill that is currently in Congress, the Commercial Facial Recognition Privacy Act, would require companies to obtain explicit user consent before collecting facial recognition data and limit sharing it with third parties.⁶⁹ Still, the bill specifically excludes any use of facial recognition by governmental bodies, including public schools.⁷⁰

If a school were to proceed and attempt facial recognition in the classroom, laws need to be enacted to regulate the collection and storage of biometric information. Schools would manage facial recognition information by serving as the repository, the same way they manage attendance records, grades, and school nurse's medical records. However, this information is arguably far more sensitive and prone to being hacked. School officials are generally not technology experts in managing data and should be trained to follow best technical practices. To be clear, these types of laws, like FERPA and COPPA, only protect information collected rather than consider the harms to privacy from collecting that information in the first place.

Putting children under the magnifying glass of facial recognition in the classroom might have some benefits, including allowing for early intervention when children do not understand the material. Nevertheless, there are other ways to achieve the same ends that better preserve privacy, such as smaller classrooms and more individualized instruction, that operate without facial recognition and constant monitoring in the classroom. To respect privacy as the right to be left alone (rather than just protecting information once collected), facial recognition must be kept outside the classroom doors.

⁶⁸ See Clare Garvie et al., *Model Face Recognition Use Policy*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), <https://www.perpetuallineup.org/appendix/model-police-use-policy>.

⁶⁹ See Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 3 (2019).

⁷⁰ *Id.*

(2) Equity

An additional concern besides privacy is equity: specifically, the harms of surveillance as it would impact children of color and those with disabilities. The current technology presents two concerns. First, facial recognition is currently unable to accurately identify black and brown faces.⁷¹ Second, facial recognition may exacerbate existing discrimination, even when the technology correctly identifies faces. The first issue is likely easier to solve through the law and technology than the second. MIT found algorithmic bias in facial recognition technology used by Microsoft, IBM, and Amazon.⁷² While the former two have taken steps to address the issues, Amazon has continued to resist attempts to address the gaps in the dataset that have led to misidentifications.⁷³ Even among a more homogenous population in South China, facial recognition is having accuracy problems, which has led schools to suspend its use during peak hours.⁷⁴ A simple regulatory solution to these problems would be to require proof of a certain level of accuracy before using the technology in schools.

The larger issue is that facial recognition in classrooms could compound an already existing problem with disparate disciplinary sanctions, a subject that the federal government addressed in a Dear Colleague Letter in 2014.⁷⁵ The letter details that federal non-discrimination requirements under Titles IV and VI of the Civil Rights Act, as well as Title II of the Americans with Disabilities Act, prohibit discriminatory discipline.⁷⁶ Additionally, the letter gives recommendations to further train school staff, collect data on discriminatory discipline, and explore alternative ways to discipline students who do not aggravate the school-to-prison pipeline. Though this

⁷¹ See Hardesty, *supra* note 54.

⁷² *Id.*

⁷³ See Matt O'Brien, *Face Recognition Researcher Fights Amazon Over Biased AI*, SPOKESMAN REV. (Apr. 12, 2019), <http://www.spokesman.com/stories/2019/apr/12/face-recognition-researcher-fights-amazon-over-bia/> (stating that Amazon dismissed concerns about a study suggesting Amazon's facial analysis misidentified darker-hued women).

⁷⁴ See Jane Zhang, *Chinese School Stops Using Facial Recognition Gates at Peak Times After Complaints About Queues*, S. CHINA MORNING POST (May 29, 2019), <https://www.scmp.com/news/china/society/article/3012301/chinese-school-stops-using-facial-recognition-gates-peak-times>.

⁷⁵ See U.S. DEP'T OF JUSTICE & U.S. DEP'T OF EDUC., DEAR COLLEAGUE LETTER (2014), <https://www2.ed.gov/about/offices/list/ocr/letters/colleague-201401-title-vi.pdf>.

⁷⁶ *Id.*

letter was rescinded by the Trump Administration,⁷⁷ nothing in the current administration's guidance prohibits individual school districts from continuing to study disparate discipline in schools and the use of alternative sanctions to suspensions.⁷⁸ However, the rescission signals that the federal government is perhaps less interested in students' civil rights and protecting them from violations because of discriminatory discipline.

It is worth noting that without data and more information, it is hard to predict whether facial recognition might actually *decrease* disparate disciplinary outcomes. It is possible that empowered with surveillance footage, children and families could better contest when discipline is unfair. School officials, with the knowledge that everything is recorded, may be more circumspect. Of course, this assumes that data kept by the schools would be readily accessible and could be easily analyzed by non-school officials. Although school records technically belong to students (with parents as the "owners" until children reach majority under FERPA), the reality is that accessing large amounts of data may present a significant issue.

Like many technological tools, facial recognition is more likely to exaggerate existing issues of discrimination rather than solve them. Technology utilizing artificial intelligence is a tool that can amplify preexisting biases because training data—the data chosen to train artificial intelligence to perform—is subject to the biases of human beings. Additionally, these biases can be harder to address because technology is often seen as neutral and beyond human prejudice.

Discrimination may also continue because of an inherent power imbalance between the holders of the data (school officials and third party aggregators) versus minority parents and their children. Racial minorities already face difficulties in navigating school systems. Putting the onus on them to interrogate facial recognition data is untenable. Increased surveillance in schools could also expose more instances of minor infractions and trigger suspensions in response to less serious violations (like using a cellphone in class or passing a note to another student) that are easier to record with facial recognition technology. A number of studies have clearly documented that school discipline is

⁷⁷ Vanita Gupta, *DeVos and DOJ Repeal Discipline Guidance that Clarifies Children's Civil Rights*, LEADERSHIP CONF. ON CIV. & HUM. RTS. (Dec. 21, 2018), <https://civilrights.org/2018/12/21/devos-and-doj-repeal-discipline-guidance-that-clarifies-childrens-civil-rights/>.

⁷⁸ *Id.*

continuing to be meted out in disparate ways, but quantifying that discrimination is an incredibly difficult task.⁷⁹

These issues are clearly harder to regulate and solve than the accuracy problem described earlier. Still, at a minimum, jurisdictions could require the collection and evaluation of data related to racial disparities, which would be the first step to addressing them. One option lawmakers could consider is racial impact statements, which thus far have been proposed to assess disproportionate impacts on minorities in the criminal justice system.⁸⁰ Essentially, racial impact statements are a tool for policymakers to assess the projected effects of laws on minorities prior to their adoption.⁸¹ Iowa, Connecticut, Oregon, and New Jersey have racial impact statements, and many other states are considering their adoption.⁸² It is still too early to assess whether racial impact statements are effective, but early reports indicate that Iowa's lawmakers are more likely to adopt laws which are projected to have a neutral or positive effect in resolving disparities in the system.⁸³ A racial impact statement could provide a vital check against perpetuating racism in schools because of surveillance.

(3) *Child Development*

Technology is an increasing part of childhood. There is no question that children switch between the physical and virtual world with much more ease than adults.⁸⁴ Still, we must consider the risks for children's overall development as technologies are used as tools of surveillance. It is very difficult to predict exactly how facial recognition in the classroom would affect a child—neither technology nor a child are

⁷⁹ See Nora Gordon, *Disproportionality in Student Discipline: Connecting Policy to Research*, BROOKINGS INST. (Jan. 18, 2018), <https://www.brookings.edu/research/disproportionality-in-student-discipline-connecting-policy-to-research>.

⁸⁰ See *State Advocacy News: Expanding Racial Impact Statements*, SENT'G PROJECT (Mar. 1, 2019), <https://www.sentencingproject.org/news/7002/>.

⁸¹ See *id.*

⁸² See *id.*

⁸³ Leah Sakala, *Can Racial and Ethnic Impact Statements Address Inequity in Criminal Justice Policy?*, URB. INST. (Feb. 23, 2018), <https://www.urban.org/urban-wire/can-racial-and-ethnic-impact-statements-address-inequity-criminal-justice-policy>.

⁸⁴ JOHN PALFREY & URS GASSER, BORN DIGITAL iii (2009) ([Children] study, work, write, and interact with each other in ways that are very different from the ways that [their parents] did growing up . . . Major aspects of their lives—social interactions, friendships, civic activities—are mediated by digital technologies. And they've never known any other way of life.”).

fixed, isolated entities in time.⁸⁵ From what we know about surveillance and how it affects the human psyche, it is clear that the constant scrutiny could have significant effects in a place where children should be free to explore, experiment, make mistakes, and learn. It may be too late to stop some instances of security surveillance at schoolyard gates, and it may be a reasonable policy decision to have some cameras because of our desire for more safety and security.⁸⁶ But with security cameras outside schools, the surveillance exposure is smaller as children would presumably only be watched while entering and exiting school grounds. The surveillance exposure and the risk of negative effects on development would be much greater with surveillance in the classroom.

If schools decide to implement facial recognition in the classrooms, a public health-based approach might inform how we might implement such a policy. A public health methodology seeks to understand the scale of the issue through research, emphasizes evidence-based solutions, monitors and evaluates such interventions, and implements them on a larger scale if successful.⁸⁷ Advocates have proposed this methodology for human trafficking, gun violence, and addiction.⁸⁸ A public health approach would, for example, examine if facial recognition particularly harms certain ages or populations, and seek to limit detrimental effects while maximizing any benefits found. Additionally, a public health methodology, which harnesses epidemiology's strengths of looking at population-based data, might be particularly well-suited for examining larger effects on our democracy because of increased surveillance in a place of learning.

On the other hand, if further studies demonstrate that facial recognition in classrooms harms the ability for children to grow into fully-fledged autonomous adults, just guardrails may not fix that issue.

⁸⁵ Tonya Rooney, *Childhood Spaces in a Changing World: Exploring the Intersection Between Children and New Surveillance Technologies*, 2 GLOBAL STUD. CHILDHOOD 331 (2012).

⁸⁶ It is a separate issue whether these cameras make us safer. For a discussion on this matter, see Jon Schuppe, *Schools are Spending Billions on High-Tech Security. But are Students Any Safer?*, NBC NEWS (May 20, 2018), <https://www.nbcnews.com/news/us-news/schools-are-spending-billions-high-tech-security-are-students-any-n875611>.

⁸⁷ Jonathan Todres, *Assessing Public Health Strategies for Advancing Child Protection: Human Trafficking as a Case Study*, 21 J.L. & POL'Y 93 (2012); Seema Mohapatra, *Unshackling Addiction: A Public Health Approach to Drug Use During Pregnancy*, 26 WIS. J.L. GENDER & SOC'Y 241 (2011); Jonathan E. Selkowitz, *Guns, Public Nuisance, and the PLCAA: A Public Health-Inspired Legal Analysis of the Predicate Exception*, 83 TEMP. L. REV. 793 (2011).

⁸⁸ Todres, *supra* note 87; Mohapatra, *supra* note 87; Selkowitz, *supra* note 87.

Similar to other policy decisions it has made to protect children, society may decide to reject facial recognition in classrooms as against society's value system. Scholars Woodrow Hartzog and Evan Selinger, who call for a wholesale ban on facial recognition, have articulated that "when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering. The law already prohibits certain kinds of dangerous digital technologies, like spyware."⁸⁹

Complete bans of facial recognition in governmental agencies, including public schools, are already occurring. San Francisco, Sommerville, and most recently Oakland, have enacted this type of law.⁹⁰ Many academics and advocates have found this technology to be so dangerous—akin to nuclear weapons or bioterror—that it is appropriate to call for a complete moratorium.⁹¹ Even those who find there are appropriate uses for facial recognition might draw the line at using the technology in classrooms. When it comes to this particular use of facial recognition, arguments related to child development are the most persuasive reasons to reject its use. The impact on individual children can, in its aggregate, put at risk a future functioning, thriving adult population in our democracy. There are reasonable uses for this technology, such as locating missing children and combating human trafficking.⁹² But taking away the sacred space of the classroom—where children should be free to learn without being surveilled—does not seem to be one of them.

⁸⁹ Woodrow Hartzog & Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

⁹⁰ See Blake Montgomery, *Facial Recognition Bans: Coming Soon to a City Near You*, DAILY BEAST (July 31, 2019), <https://www.thedailybeast.com/facial-recognition-bans-coming-soon-to-a-city-near-you>.

⁹¹ Evan Greer, *Don't Regulate Facial Recognition. Ban It*, BUZZFEED NEWS (July 18, 2019), <https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it>.

⁹² Anthony Cuthbertson, *Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology*, INDEPENDENT (Apr. 24, 2018), <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>; Alexandra Ossola, *AI Tool Helps Law Enforcement Find Victims of Human Trafficking*, FUTURISM (Apr. 16, 2018), <https://futurism.com/ai-tool-law-enforcement-stop-human-trafficking>.

V. CONCLUSION

If we are trying to promote pro-social behavior, such as paying attention in class, research demonstrates that creating a bond of trust between adults and children is much more effective than surveillance in encouraging children to communicate and learn freely.⁹³ Trust requires relying on another's good will, which makes us vulnerable; trust can always be broken.⁹⁴ It is ultimately a risky endeavor to trust rather than surveil someone, but it is also the true basis of any meaningful relationship. Surveillance undermines this bond of trust by making it clear that all students are suspects and under scrutiny, which disrupts the relationship of trust between teacher and student.⁹⁵

Too often, policy has assumed a reactive rather than proactive position with respect to new technologies affecting children. While some schools in China have already implemented facial recognition in classrooms, there is still time for schools and legislators in the West to formulate policy on facial recognition in the classrooms. Certain segments of our society, including the cities that have passed and are considering outright bans, have decided that the risks of facial recognition are too high. Even for those jurisdictions more willing to consider it, such technology warrants further research about how surveillance can affect children, the classroom environment, our democracy, and racial inequities already present in our schools and justice system. We have the responsibility to be vigilant about protecting our children and preserving their childhood—including their play, imagination, and mind-wandering.

⁹³ Margaret Kerr & Hakan Stattin, *What Parents Know, How They Know It, and Several Forms of Adolescent Adjustment: Further Support for a Reinterpretation of Monitoring*, 36 DEVELOPMENTAL PSYCHOL. 366, 366–80 (2000) (that over-monitoring leads to resentment); Julien Bureau & Genevieve Mageau, *Parental Autonomy Support and Honesty: The Mediating Role of Identification with the Honesty Value and Perceived Costs and Benefits of Honesty*, 37 J. ADOLESCENCE 225, 225–36 (2014). <http://www.mapageweb.umontreal.ca/mageaug/Articles/Bureau%20&%20Mageau%202014.pdf> (finding that providing more autonomy rather than control to youth promotes honesty and trust).

⁹⁴ Annette Baier, *Trust and Antitrust*, 96 ETHICS 231, 234 (1986).

⁹⁵ Martin R. Gardner, *Student Privacy in the Wake of T.L.O.: An Appeal for an Individualized Suspicion Requirement for Valid Searches and Seizures in the Schools*, 22 GA. L. REV. 897, 943 (1988).